

PCI DSS Compliance Services

Protect your cardholder data and **secure your business**



**Working closely with our customers as
their end-to-end PCI compliance partners**

Store, transmit, process and protect your customer card data securely

Meeting regulatory compliance can be a complex minefield without the right level of knowledge or technical support. Secure your business and cardholder data, mitigate risk and meet your PCI DSS compliance requirements with Claranet Cyber Security.

Your end-to-end PCI compliance partner

In addition to our accreditations as Payment Card Industry Qualified Security Assessors and a PCI Approved Scanning Vendor we provide a complete end-to-end service for all your PCI needs. From gap analysis to risk assessments, from milestone assessments to onsite resources to help drive PCI DSS projects forward, we can help.



Non-compliance: **the numbers**

In cases of non-compliance fees, payment brands fine the acquiring banks who then pass this onto their merchant customers. In our experience, these monthly fees can be anything from £50 per Merchant ID, to thousands of pounds if based on a percentage of the transaction amounts. For many businesses this can be a damaging amount. In some cases, non-compliance could also mean the business is eventually banned from accepting cards.



Qualified Security Assessor

Technically, we are a PCI Qualified Security Assessor Company and we offer specialist consultancy for compulsory PCI DSS compliance. PCI Data Security Standard (PCI DSS) compliance is mandatory for organisations involved in the storage, processing or transmission of cardholder data. However, it is a complex process or can impact upon and entities cardholder data.

Why use our assessors:

- We are qualified to offer specialist consultancy for compulsory PCI DSS compliance
- We can also add value by offering in-house technical expertise to further improve network and information security for Retail, Financial Services, e-Commerce organisations and service providers



Approved Scanning Vendor

An Approved Scanning Vendor is an organisation with a set of security services and tools to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS. The scanning vendor's ASV solutions are tested and approved annually by the PCI SSC. before an ASV is added to PCI SSC's List of Approved Scanning Vendors.

Why use Claranet Cyber Security for PCI scanning?

- **Low cost** - Competitively priced per IP address per quarter
- **Qualified personnel** - Highly skilled and experienced security engineers
- **Maximum quality** - Engineers use manual and automated techniques to maximise service
- **Customer service and support** - We go further than other providers. Assistance will be provided to:
 - Advise on the recommended scope based on current network architecture
 - Prioritise the solution and mitigation of identified issues
 - Apply corrective actions in line with the PCI DSS







5 stage approach to meeting PCI DSS

We continually work with clients of all sizes at various stages of their PCI DSS journeys. We have developed a 5-stage approach designed to help organisations manage their PCI DSS projects and ongoing PCI DSS compliance.

These stages follow an organisation's journey from the start of a PCI DSS project towards becoming PCI DSS compliant and then maintaining compliance on an ongoing basis. Claranet Cyber Security can also assist if you are part way through a PCI DSS project.



Our accreditations

Claranet Cyber Security continually invests in hiring the most experienced, highly trained teams in the industry. A core part of delivering the best service is our commitment to being fully accredited across all the major standards in IT security. These include:



Protect your cardholder data
and **secure your business.**

Call us today:

01924 284 240





claranet[®]
cyber security